Request for Information (RFI) - E-Discovery Solution

Background and Scope

The Federal Bureau of Prisons (BOP) is an agency of the Department of Justice (DOJ). It consists of 121 institutions throughout the United States, including Hawaii and Puerto Rico; 6 regional offices, a Central Office (headquarters), 2 staff training centers, and 26 Residential Reentry Management offices (previously known as community corrections offices).

The BOP is responsible for the custody and care of approximately 219,000 Federal offenders. Approximately 81 percent of these inmates are confined in Bureau-operated facilities, while the balance is confined in secure privately managed or community-based facilities and local jails. More information about the agency can be found on the BOP's public site, www.bop.gov.

The BOP's Office of General Counsel (OGC) provides legal advice, representation and assistance to BOP and Federal Prison Industries (FPI) officials. The BOP's OGC is comprised of approximately 385 staff members including, but not limited to, attorneys, paralegals, and legal assistants. OGC staff are located in each of the BOP's 6 regional offices, various Consolidated Legal Centers (legal offices located at BOP institution's), and Central Office (which includes the Employment Law Branch, Commercial Law Branch, Litigation Branch and FOIA/Remedies Processing Branch).

The BOP requires an e-discovery solution to respond to internal and external regulatory inquiries/investigations and litigation. The types of litigation or investigations the BOP deals with vary greatly. Additionally, some of our attorneys represent the BOP in court or before administrative judges, while others work with the United States Attorney's office to represent BOP staff.

Purpose

The Federal Bureau of Prisons is seeking information about E-discovery Solutions that can assist the BOP in responding to litigation and/or regulatory investigations. The BOP is seeking a solution that can assist in (1) identification, preservation, and collection; (2) processing, analysis, and review; and (3) production of discovery. Currently, the BOP does not have a centralized or formal mechanism for the e-discovery process and all e-discovery is conducted and processed internally.

Information provided by responsive vendors will be used to further refine the BOP's specifications for the eventual solicitation/acquisition for such a system. The specific questions outlined in this Request for Information should be answered by vendors in as much detail as possible, including describing actual hardware, any necessary software, any peripherals required, and any configuration required to support the solution. A response that simply states that the vendor's solution is compatible with the specified requirement will be considered non-responsive for that section.

Vendors should propose a solution which addresses the functional, technical and security requirements identified in the RFI. Any proposed solution should also include discussion of any mobile capabilities or limitations to ensure that the system can be accessed either via a desktop or mobile interface. The

vendor's ability to comply with specific DOJ IT security requirements is also a key consideration and those requirements are described in various sections below.

The BOP may schedule an onsite, follow-up demonstration at BOP headquarters of select systems for vendors to provide more detailed information and display system functionality. If web/virtual conferencing is used for a remote demonstration, the following solutions would be supported: Cisco WebEx, Citrix GoToMeeting or Adobe Connect and the vendor should account for at least ten (10) possible connections.

SYSTEM SOFTWARE/HARDWARE AND PERFORMANCE REQUIREMENTS

Vendors must be able to demonstrate the ability to meet technical and system performance requirements through documentation, current client references and/or online demonstrations of the applicable system.

Hardware Requirements

The vendor will provide the minimum server hardware specifications required to support a typical BOP site, as well as specifications for an enterprise system accounting for BOP's size and geographic scope. The vendor may be asked to provide a network architecture diagram which describes proposed network and system communications and interfaces.

A. Database Components and Integration

1. Is system capable of doing a real-time or automated scheduled sync of records (i.e. can it take advantage of a web service or automated pull of data from an enterprise data store)?
2. Can system uniquely identify records and does it have an audit capability to identify duplicates?
3. Specify the database technology used (IBM DB2, Microsoft SQL Server, Oracle, etc.)
4. Does database system design support clustering and failover?

B. Network Hardware Specification

A. Does the system support a multi-tier architecture with the ability to fully employ load-balancing and failover capabilities of the application?
B. If server-based:
    a. Is the system capable of being installed as a high availability solution on HP servers, leveraging 64-bit processors?
C. Is the system capable of operating on virtualized servers using Microsoft Hyper-V virtualization environment?
D. If mainframe-based:
    a. Is the system capable of running on IBM zEnterprise hardware, including making use of System z Application Assist Processors (zAAPs) for Java-based workloads?
E. If cloud-based:
    a. Is the system capable of being hosted in customer's cloud environment?

C. Network Software Specifications

1. Does the system provide authentication via an LDAP ver.3 interface? (Note: if only Microsoft Active Directory is supported vs. full LDAP-compliance, please indicate.)
2. Is the system capable of being PIV-enabled to permit login via the use of an HSPD-12 compliant card?

D. System Software Specifications

1. Is system web-based (i.e., no proprietary client agent software required)?
2. Is system capable of single sign-on to the user interface (i.e. separate logins are not required to access application subsystems)?
3. **Specify how many concurrent users system supports;**
4. Is customization of the software possible by the customer?
    a. If yes, describe what user interfaces and modules the customer can modify;
    b. If yes, does customization occur at the system-level or do users have the ability to modify their individual user interfaces?
5. Please describe the largest customer who is operating your software (describe geographic dispersion, number of users, number of offices, departments or business units) and whether/how it is being used by government agencies.

E. Software Upgrades and Patches

1. What is the process and cycle for software enhancements (e.g. if a customer requests a new feature or software modification, is there a threshold requirement as to the number of other customers requesting the same before development occurs? Do upgrades occur on a regular schedule)?
2. How soon after a security vulnerability (e.g. a Common Vulnerabilities and Exposures identified software flaw or misconfiguration) is identified, will you provide a patch or fix?

F. Workstation Specifications

1. Is system compatible with Internet Explorer 11? (specify any other browsers which are compatible);
2. Is system compatible with Windows 7 or higher (specify if 32-bit only or 64-bit)?
3. Does system require additional client software to be installed (e.g. JRE, Microsoft Silverlight, ActiveX controls, Adobe Flash, etc.)? If yes, specify products.

G. Cloud Specifications

1. Is cloud/system FEDRAMP-certified?
    a. If yes, specify the cloud service tier (IaaS, SaaS, PaaS);
    b. If no, is certification under development? (specify planned date for certification);

System Security Specifications

A. Web and Configuration Security

1. If system is web-based, does it support HTTPS connections of at least 128-bit TLS 1.0 encryption?
2. Does system security configuration comply with guidelines from the National Institute of Standards and Technology Special Publication (SP800) series, including user audit trail capabilities?

NOTE: If vendor remote access for application maintenance is required or implemented, it must comply with DOJ IT security requirements (e.g., security background checks, US citizenship, etc.).

B. WAN/Telecommunications

1. Does system support the IPv6 network configuration?
2. Can system operate with an internet proxy for any required internet access?

For communications outside of the BOP network, AES 128-bit encryption is the minimum acceptable with AES 256 preferred.

C. Role and Access Management:

1. If system supports a single, unified database (See "Hardware Requirements | D. Database Software Specification", above), does system segregate access to data by site location and by user role (e.g. users at the Federal Medical Center in Rochester, Minnesota can only access records for staff at FMC Rochester and not data for staff at FCI Cumberland)?
2. Does system support tiered-role privileges that distinguish between users and administrators and their authorized functions?
3. Does system require unique user authentication for each authorized user (i.e., user passwords cannot be shared and one user cannot login for all staff to access the system)?

D. Personnel Security

Any individual who desires to access or develop a BOP-networked system:

- Must undergo an OPM Moderate-Risk Background Investigation (MBI). This requirement applies to anyone physically and directly accessing a networked device, or via remote access.
- Must be a US citizen.

Is vendor capable of complying with the above personnel security requirements?

E. Licensing Specifications

1. How is software licensed? (e.g. by CPU core, by users, etc.; please specify)
    a. If by user, does licensing distinguish between general users and administrators?
2. How is licensing monitored? (e.g. system only allows for specified user count or system allows additional users to be added and vendor performs "true up" at annual cycle, etc; please specify).

Solution Profile

Please use the following table to indicate the areas in the Electronic Discovery Reference Model (EDRM) that are supported by your e-discovery solution(s). Please enter the product name that supports each EDRM phase. If the EDRM phase is not supported by your e-discovery solution(s) directly, but you have one or more 3rd party vendor partnerships that support those phases, please name and describe the nature of these relationships.

Solution Profile	Y/N	Name of Product(s) Supported by Vendor	Name of 3rd Party & Description of Partnership
Please indicate the areas in the EDRM that are supported by your e-discovery solution (s):			
Identification			
Preservation			
Collection			
Processing			
Analysis			
Review			
Production			

Functional Requirements

For each requirement, indicate whether the proposed solution(s) supports the requirement. If more clarification is needed, provide it in the Vendor Response section.

Requirement	Requirement Supported (Y/N)	Vendor Response
IDENTIFICATION		
Please describe how your solution identifies and searches for data		
PRESERVATION		
Please describe how your solution preserves data and prevents spoliation		
Support for legal holds		
Support for multiple searches used to place and remove holds per matter		
Support for multiple legal holds on a record without need for copies		
Support for ability to remove legal holds on a record per matter		
Support for in-place legal hold on existing Content		
Support for controlled suspension of automatic deletion routines		
COLLECTION		
Support for collection of multiple searches to place records into a legally defensible, secured location for each matter		
Support for collection of files from shared directories/file shares, desktops and laptops attached to corporate network		
Collection can occur in such a way that business operations are not interrupted		
PROCESSING		
Provides statistical and graphical analysis of collected data based on custodian, date range, and file type prior to processing		
Ability to filter collected data by custodian, date, file type, and file size prior to processing		
Ability to filter collected data by customer defined known file lists prior to processing		
Ability to process (extract text and metadata) from a large variety of file types (specify which types)		
Ability to de-duplicate records and data of a single custodian across multiple data		

stores and across all custodians		
Provides a pre-processing scan of all documents to detect and repair file-level errors prior to full processing		
Support for processing reports to understand file errors, warnings, and key processing metrics such as de-duplication rates, total # of messages and loose files, and average document size		
Time-zone settings		
Support extraction of attachments from emails and ability to process attachments as separate documents that are associated with the original email message.		
System maintains metadata between original files and attachments		
Provides capability for metadata extraction making it available for review		
Ability to later add information to an index without re-indexing the entire case dataset		
Support processing of nested email attachments (e.g. the solution can process all documents in the case of an email which contains a .msg attachment which contains a zip file attachment which contains a word document)		
Ability to identify and report on encrypted and password protected files		
ANALYSIS		
Support for nesting multiple combinations of Boolean search terms and parameters into expressions including AND, OR, NOT, etc.		
List the searchable file formats		
Support for all analysis features to operate on and across the entire matter, including matters up to 5 million documents. Please detail what features do not analyze content across the entire case data set at once		
Supports stemming and literal searches		
Supports search of content in tags or document notations		
Support for searches by document ID, source location, custodian or processing batch		
Support search by senders, recipients, urgency, and direction (e.g., internal email only) of email		
Support search by attachment content or type		

Describe how your solution helps us with Rule 26(f)		
Describe how your solution ensures the defensibility of keyword selection and searching procedures to avoid e-discovery defensibility issues		
Provides automatic documentation and/or reporting of executed searches and keyword variation selections		
Support real-time and iterative sampling of search results		
Ability to preview search results prior to running searches to remove obvious false positives		
Support for relevance ranking: Retrieved documents that most closely satisfy the query criteria should be listed or ranked above those that match less exactly. Ranking should also place a higher priority on matches in a title or subject than on those in body text		
Use of directory information such as names, e-mail addresses, and department groupings to extend the values of certain metadata fields, such as message recipients, or create new metadata, such as departments creating or receiving content		
Provides ability to visually track e-mail threads for responses based on content and metadata, not just metadata		
Ability to group documents and e-mails together that pertain to the same/similar topic		
Ability to identify and group documents based on language		
Ability to identify and group documents by frequently found nouns or noun phrases		
Ability to organize and group related loose files for analysis		
Ability to organize and group related custodians for analysis		
Provides hit highlighting in text, metadata, and attachments		
Cull-down & Filtering: Ability to filter documents across the entire case by tag, sender domain, sender group, sender name, recipient domain, recipient group, recipient name, document type, custodian, and language type and displays exact hit counts across the entire search result set for every filter		
REVIEW		

Allows users in various offices throughout U.S. to work on the same cases		
Ability to divide records so each reviewer is assigned a specific range or percentage of records, or by the source or significance of a subset of records (including Role Based Access Controls)		
Ability to organize documents intended for review into access controlled nested folders		
Ability to customize tags, issue codes, and tagging rights		
Support for hierarchical tagging structures that define and require sub-tags based on parent tags		
Support for tagging or classification of documents via a single mouse click		
System provides ability for individual and bulk categorization and tagging		
Ability to tag privileged communication and create privilege log		
Provides ability to view documents within a native viewer, abdicating the need for reviewers to load applications on their workstations		
Support for hit highlighting of searched terms during review in native viewer or HTML format		
Support for redaction of text, areas within a document, and entire pages		
Provides redaction verification capabilities		
Provides find-and-redact functionality		
Identifies and displays items related to the document in review		
Provides review progress and productivity analysis for each reviewer		
Automatically documents reviewer actions such as login, logout, search, tag, print, and export		
PRODUCTION		
Support for individual products sets and batch export		
Support for export to HTML		
Support to “un-duplicate” data by custodian on export. Change to: Support to “reduplicate” documents by custodian on export		
Support for export to Concordance file format		
Support for export to Relativity file		

Support for export to EDRM XML compatible formats – Please describe specification and version		
Support for producing documents one at a time or in batch		
Ability to organize production sets using a folder based structure		
Support for produced redactions, where text is secured from unauthorized display, search, and review.		
Support for custom header, footer, and watermark labeling of documents in image-based production		
Support for Bates stamping		
Support for reporting on processing statistics, case progress (# of docs reviewed, tagged, etc).		

1. What other functions does the system support (e.g. does it support mobile access? please specify the additional features)

2. Does Vendor provide application support and training? Please specify.

3. Does your solution function across a WAN?

4. Describe how many cases your solution can handle and the amount of documents.

5. Describe your solution's storage requirements and capabilities.

6. Describe your solution's ability to provide audit history logs, which include a means of reporting on searches by custodian, operator, keyword, phrase, concept and matter.

Additional Notes: The application environment should be capable of supporting a test environment, separate from the production region, to facilitate troubleshooting and new test/process development.

The vendor should also specify peripheral components which are included in the proposed solution.